УДК 343.2/.7
DOI https://doi.org/10.32850/sulj.2022.4.1.12

# ПОРІВНЯЛЬНИЙ АНАЛІЗ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ КІБЕРПРОСТОРУ КРАЇН БАЛТІЇ ТА УКРАЇНИ

***Думчиков М. О.***

*Метою статті є здійснення порівняльно-правового аналізу кіберзлочинності як однієї із загроз національній безпеці країн Балтії та України. Досліджено особливості профілактики та протидії кіберзлочинності в країнах Балтії та Україні. Визначено поняття «кримінальне правопорушення у кіберпросторі» та здійснено відмежування від суміжних понять, зокрема «комп'ютерне кримінальне правопорушення» і «правопорушення у сфері комп'ютерної інформації». Так, у статті під кримінальним правопорушенням у кіберпросторі розуміється будь-яке суспільно небезпечне, винне діяння, вчинене в кіберпросторі суб'єктом кримінального правопорушення.*

*Автор наголошує, що нині ми живемо в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людини і держави. Але людство, поставивши собі на службу телекомунікації та глобальні комп'ютерні мережі, не передбачило, які можливості для зловживання створюють інформаційні технології. Особливу увагу зосереджено на кримінальних правопорушеннях у кіберпросторі Латвії, Литві та Естонії. Описано основні види кримінальних правопорушень у кіберпросторі, відповідальність за вчинення яких передбачена Розділом XVII Кримінального кодексу України.*

*Авторами проаналізовані основні нормативно правові акти з питань регулювання кібербезпеки країн Балтії та України, визначені їх основні недоліки та способи реформування окремих нормативних питань, пов'язаних із кібербезпекою.*

*Наголошено на основних загрозах, які ставлять виклик країнам Балтії та України, зокрема, серед основних загроз вбачаємо пропагандистку діяльність Російської Федерації в інформаційній сфері та її деструктивну діяльність в кіберпросторі. Наведено дані департаментів поліції країн Балтії щодо дискредитації держав у засобах масової інформації, щодо порушення прав і свобод російськомовних громадян.*

*Визначено, що з метою протидії кримінальним правопорушенням у кіберпросторі країнам Балтії та Україні необхідно постійно підвищувати безпеку інформаційних систем, розвивати сучасні інформаційні технології, удосконалювати законодавство та розширювати міжнародне співробітництво у сфері забезпечення кібербезпеки. Також вважаємо за потрібне посилення санкцій в інформаційному середовищі щодо подальшої пропаганди Російської Федерації.*

***Ключові слова:*** *кіберзлочин, кіберзлочинність, протидія кримінальним правопорушенням у кіберпросторі, міжнародна співпраця, кримінальні правопорушення у кіберпросторі, кіберпростір, види кримінальних правопорушень у кіберпросторі.*

**Dumchykov M. O. Comparative analysis of criminal and legal protection of cyberspace in the Baltic States and Ukraine**

*The purpose of the article is to conduct a comparative legal analysis of cybercrime as one of the threats to the national security of the Baltic states and Ukraine. Peculiarities of cybercrime prevention and countermeasures in the Baltic countries and Ukraine have been studied. The concept of 'criminal offense in cyberspace' was defined and a distinction was made from related concepts, in particular 'computer criminal offense' and 'offense in the field of computer information'. Thus, in the article, a criminal offense in cyberspace means any socially dangerous, culpable act committed in cyberspace by the subject of a criminal offense.*

*The author emphasizes that today we live in the era of the information society, when computers and telecommunication systems cover all spheres of human and state life. But humanity, having put telecommunications and global computer networks at its service, did not foresee the opportunities for abuse created by information technology. Special attention is focused on criminal offenses in cyberspace in Latvia, Lithuania and Estonia. The main types of criminal offenses in cyberspace are described, the responsibility for their commission is provided by Chapter XVII of the Criminal Code of Ukraine.*

*The authors analyzed the main normative legal acts on the regulation of cyber security of the Baltic countries and Ukraine, identified their main shortcomings and methods of reforming certain regulatory issues related to cyber security.*

*The main threats that challenge the Baltic countries and Ukraine are emphasized, in particular, among the main threats we see the propaganda activities*

*of the Russian Federation in the information sphere and its destructive activities in cyberspace. Data from the police departments of the Baltic states regarding the discrediting of the states in the mass media and the violation of the rights and freedoms of Russian-speaking citizens are provided.*

*It was determined that in order to combat criminal offenses in cyberspace, the Baltic States and Ukraine need to constantly improve the security of information systems, develop modern information technologies, improve legislation and expand international cooperation in the field of cyber security. We also consider it necessary to strengthen sanctions in the information environment regarding further propaganda of the Russian Federation.*

***Key words:*** *cybercrime, cybercrime, combating criminal offenses in cyberspace, international cooperation, criminal offenses in cyberspace, cyberspace, types of criminal offenses in cyberspace.*

**Постановка проблеми.** На перший погляд питання кримінально-правової охорони кіберпростору достатньо врегульоване, однак саме питання протидії має декілька серйозних прогалин, більшою мірою це стосується саме недосконалості кримінального процесу. Сьогодні ця правова сфера активно розвивається, реформи направлені на посилення правового забезпечення кібербезпеки та протидії кримінальним правопорушенням у кіберпрострі. Визначено основні види кіберзагроз, напрями профілактика та протидії кіберзлочинності в країнах Балтії та України.

**Актуальність теми.** У період збройної агресії Російської Федерації питання забезпечення кібербезпеки постає доволі жорство. Перед пострадянськими країнами та Україною зокрема постають нові виклики, які перш за все по'вязані із протидією кримінальним правопорушенням у кіберпросторі, які в цей період мають неабияку динаміку зростання. В період збройної агресії кібернетична структура країн Балтії та України переживає найбільшого негативного впливу як з боку спеціалізованих організацій, так і з боку звичайних користувачів кіберпростору. Варто зауважити, що шкода від кримінальних правопорушень у кіберпросторі причиняється не тільки обороноздатності нашої держави, але і окремим громадянам, тобто має різнорідні об'єкти свого посягання.

**Аналіз наукових досліджень.** Проблематикою забезпечення кібербезпеки в країнах Балтії та України опікувалися К. Марія, О. Ільченко, О. Резнік, А. Голуб, В. Шаблистий, Д. Нікулеско, М. Гуцалюк та інші.

**Метою** цієї статті є здійснення порівняльно-правового аналізу кіберзлочинності як однієї із загроз національній безпеці країн Балтії та України та окреслення основних засобів протидії цьому суспільно небезпечному діянню.

**Виклад основного матеріалу.**

Як відомо, в середині 70-х рр. минулого століття в суспільстві стартувала техніко-економічна хвиля, що базується на інформаційно-комунікативних технологіях. Минуло кілька десятиліть, і сьогодні ми можемо констатувати, що інформаційно-комунікативні технології проникли практично в усі сфери людської життєдіяльності. В останні роки як у загальний, так і в професійний лексикон громадян увійшли нові терміни: інформатизація, цифрові технології, цифровізація, цифрова реальність, віртуальна реальність, інформаційно-комунікативний простір та кіберпростір. Кримінальні правопорушення в кіберпросторі – це небезпечні для суспільства діяння, здійснювані умисно або з необережності, які загрожують безпеці комп'ютерної інформації та здатні заподіяти шкоду благам, охоронюваним законом (прав особистості, відносин власності і т.д.)

Активне зростання кіберзагроз в сучасному суспільстві ставить перед кожною державою надзвичайно актуальне завдання – необхідність забезпечення інформаційної безпеки. Щорічна світова оцінка стану даного типу злочинності викликає побоювання у зв'язку з низьким рівнем захищеності громадян сучасного інформаційного суспільства, при цьому спектр проблем досить широкий – від технічної незахищеності до уразливості систем забезпечення роботи, призначених для проведення операцій з грошовими коштами [1, с. 182].

Не дивлячись на те, що вивчення даної проблеми ведеться не одне десятиліття, тим не менш не досить повно сформовано поняття «кримінального правопорушення у кіберпрострі», що дозволяє широко «розгортатися» злочинним угрупуванням. Суспільна небезпека даної проблеми визнана на міжнародному рівні, що виражається у відповідних рішеннях міжнародних організацій. В першу чергу, це визначення самого поняття «кіберзлочинність». Воно дано в рекомендаціях експертів ООН: «Кіберзлочинність – це будь-який злочин, який може відбуватися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі або проти комп'ютерної системи або мережі» [2].

Нині в кримінальному кодексі країн Балтії (Естонії, Литва, Латвія) немає визначення поняття «кримінальне правопорушення у кіберпросторі». Так само визначення «кримінального правопору-

шення у кіберпросторі» відсуне у кримінальному кодексі України, однак в Законі України про «Про основні засади забезпечення кібербезпеки України» кримінальних правопорушень у кіберпросторі визначається як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано кримінальним правопорушенням міжнародними договорами України [3].

Крім зазначених визначень, існує перелік так званих «комп'ютерних кримінальних правопорушень», сформований Радою Європи. У даній Конвенції описуються 4 види комп'ютерних кримінальних правопорушень, які визначаються як протиправні діяння проти конфіденційності, цілісності і допустимості комп'ютерних даних і систем [4]:

1) незаконний доступ (ст. 2);

2) нелегальне перехоплення (ст. 3);

3) втручання в дані (ст. 4);

4) втручання в систему (ст. 5)

5) зловживання пристроями (ст. 6)

7) підробка, пов'язана з комп'ютерами (ст. 7)

8) шахрайство, пов'язане з комп'ютерами (ст. 8)

Більшість кримінальних правопорушень у кіберпросторі характеризуються такими особливостями: 1) підвищена скритність скоєння кримінального правопорушення; 2) транскордонний характер кримінальних правопорушень у кіберпросторі, при якому злочинець, об'єкт кримінально протиправного посягання і потерпілий можуть перебувати на територіях різних держав; 3) можливість скоєння кримінального правопорушення в автоматизованому режимі в декількох місцях одночасно; 4) необізнаність потерпілих про те, що вони піддалися кримінально-протиправному впливу; 5) дистанційний характер кримінально-протиправних дій в умовах відсутності фізичного контакту злочинця і потерпілого; 6) неможливість запобігання і припинення кримінальних правопорушень даного типу традиційними засобами.

Безпека в сучасних умовах стає категорією, якою оперують вчені багатьох гуманітарних та суспільних дисциплін, в тому числі соціальної філософії та політології, філософської антропології та соціології, соціальної психології та міжнародного права. Безпека має величезне значення в глобальній політиці та міжнародних відносинах, її різні аспекти регулюються на міжнародно-правовому рівні. Застосування основ теорії безпеки дозволить нам розглянути як цивільні, так і силові підходи до питань забезпечення кібербезпеки і сприйняття можливих загроз і їх джерел. Спробуємо дослідити політику кібербезпеки деяких країн Балтії. Існують різноманітні доктрини, які розглядають питання кібербезпеки.

Парадигма національної безпеки відображає традиційну роль держави в забезпеченні безпеки кордонів країни і дотриманні верховенства права [5, с. 14]. Кібербезпека нині визнається основоположною для державної військової та економічної безпеки, її необхідність виправдовується традиційними аргументами національної безпеки, заснованими на захист держави.

Серед європейських країн, що займаються реалізацією політики кібербезпеки, цікавим є досвід Естонії. Державою розроблені і прийняті стратегічні документи в цій сфері, створені відповідні інституційні структури. Стратегічне планування забезпечує згуртованість всієї архітектури кібербезпеки. У 2008 р. Естонська Республіка одна з перших в світі прийняла Національну стратегію кібербезпеки, вписану в рамки міжнародного права [6]. Естонія приступила до створення умов, що полегшують використання інформаційно-комунікаційних технологій і розробку «розумних рішень». Міністр закордонних справ Естонії М. Кальюранд, виступаючи в 2016 р. в Брюсселі на конференції з управління Інтернетом в Європі «EuroDIG (EuropeanDialogueonInternetGovernance)», заявила про те, що «розвиток кібербезпека повинні стати частиною повсякденного життя людей, а не «люксовим товаром» [7].

З 2011 р відповідальність за координацію політики в області кібербезпеки Естонії в цілому перейшла від Міністерства оборони до Міністерства з економічних питань та комунікацій. Рада з кібербезпеки Естонії, будучи міжвідомчим органом, надає підтримку міжвідомчої співпраці на стратегічному рівні і нагляду за реалізацією цілей стратегії кібербезпеки країни. Міністерство оборони є координаційним органом для кібернетичної оборони в області національної оборони. З 2008 року у складі сил оборони Естонії знаходиться Центр передового досвіду НАТО з кібероборони – Міжнародна військова організація, яка зосереджує свої зусилля на розширенні можливостей кібернетичної оборони НАТО і країн-партнерів. НАТО офіційно визнало кіберпростір операційним середовищем і таким чином прирівняв існуючі в ньому загрози до військових загроз.

У 2017 року в Таллінні був створений Об'єднаний центр передових технологій з кібероборони НАТО (NATO CooperativeCyber

DerenceCentreofExcellence) – флагман європейської кібербезпеки. Центр отримав акредитацію НАТО, налічує 20 учасників – 17 членів НАТО і три держави партнера. У ньому трудяться і військовослужбовці, і цивільні особи, і представники Уряду Естонської Республіки. Робота Центру сфокусована на трьох основних напрямках: дослідження, тренування, навчання. Основне завдання Центру – тренування фахівців з різних країн, які забезпечують безпеку в національному кіберпросторі. За словами директора Центру М. Майгре, «найнебезпечнішими кіберзагрозами є ті, які підтримуються на державному рівні» [13]. Центр щорічно проводить найбільші в світі кібернавчання «LockedShields» для експертів в області кіберзахисту. У 2017 року в Таллінні відбулися навчання КІБЕРЦЕНТР НАТО під назвою «Зімкнуті щити» (LockedShields 2017), в яких взяли участь близько восьмисот фахівців з 25 країн у сферах інформаційних технологій, міжнародного права, спеціальних служб, науки і ЗМІ. Співробітниками Центру розробляється доктрина з кіберзахисту, тобто єдиний алгоритм дій у разі кіберзагроз. Планується, що нова доктрина буде схвалена НАТО в 2019 г. Все це свідчить про активізацію роботи з віртуалізації безпеки, включаючи військову.

У Латвійській Республіці прийнята Стратегія кібербезпеки на період 2014–2020 рр., в якій розглядаються загрози, пов'язані з безпекою інформаційно-комунікаційних технологій в кіберпросторі і дається прогноз по ризиках кібербезпеки на майбутнє. Відповідно до Закону Латвії про безпеку інформаційних технологій визначаються основні вимоги щодо безпеки для державних і муніципальних установ, постачальників загальнодоступних електронних комунікацій [8]. Два документи віддзеркалюють комплексний підхід до захисту безпеки в кіберпросторі і національної безпеки Латвії в цілому. В рамках цієї політики визначені такі напрямки діяльності: управління кібербезпекою, правопорядок в кіберпросторі і зниження рівня кіберзлочинності, освіта суспільства і дослідницька робота в цій сфері, міжнародна співпраця.

У Литовській Республіці питання нормативно правового регулювання кібербезпеки пройшло тривалу еволюцію від створення установ, що займаються питаннями кібербезпеки, до прийняття закону про кібербезпеку. За Глобальним індексом кібербезпеки, складеним Міжнародним союзом електрозв'язку, Литва займає 57-е місце. В цілому цей індекс відображає рівень кіберзахищеності держав і зусилля, які докладає конкретна країна для поліпшення цього показника. До слабких сторін в литовській кібербезпеки можна віднести: 1) низькі стандарти в організаціях, недостатній рівень суспільної ос ведомленності; 2) відсутність заходів стимулювання і міждержавних домовленостей .

Влада Литви не раз виявляла бажання взяти на себе роль лідера в питаннях кібербезпеки як в Європейському союзі, так і у співпраці з США. У червні 2018 Сейм Литви прийняв зміни до закону про кібербезпеки. Отже, огляд національних стратегій кібербезпеки в країнах Балтії показав, що їхні стратегії кібербезпеки стають комплексними і всеосяжними. Ці стратегії охоплюють економічні, соціальні, міжнародно-правові, правоохоронні, військові аспекти кібербезпеки. Варто зазначити, що держави Балтії визнають взаємозв'язок між сферою кібербезпеки і національною безпекою та усвідомлюють, що проблеми кібербезпеки, такі як руйнування системи інформаційно-комунікаційних технологій або критичної інфраструктури, можуть завдати шкоди національній безпеці і дієвому функціонуванню економіки держави.

Кожна з розглянутих країн Балтії має свою стратегію кібербезпеки і відповідні закони для вирішення проблем кібербезпеки. Естонія, Литва і деякою мірою Латвія мілітарізують питання кібербезпеки. Ця тенденція піднімає кібербезпеку до рівня національної безпеки і фокусується на захисті державних ресурсів інформаційно-комунікаційних технологій. Зокрема, Естонія та Литва схильні ідентифікувати проблеми кібербезпеки як загрозу нормальному функціонуванню держави і виявляти напад з боку іноземних держав як найбільш небезпечні джерела таких загроз. У цих державах відповідальність за нейтралізацію кіберзагроз передається силовим установам.

Розглянувши сучасні тенденції кібербезпеки країн Балтії, пропонуємо розглянути стан кібербезпеки в Україні. На думку аналітиків, кількість кримінальних правопорушень у кіберпросторі в Україні до 2024 року загрожує вирости в чотири рази, а загальні втрати можуть перевищити кілька мільйонів доларів. Щоб захиститися від хакерів, в економічно розвинених країнах різко збільшуються витрати на кібербезпеку.

В Україні кіберпростір регулюється великою кількістю різних актів. До основних варто віднести Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про телекомунікації», «Конвенція про кіберзлочинність», а також Кримінальний і Кримінальний Процесуальний Кодекси України [9]. Зазначені

закони дають визначення усьому кіберпростору та окремим його ланкам, а також регулюють окремі питання його функціонування, однак закон про основні засади забезпечення кібербезпеки, крім того, також встановлює принципи та особливості боротьби з кіберзлочинністю. «Конвенція про кіберзлочинність» дуже детально регулює питання протидії кіберзлочинності, особливо на міжнародному рівні [4]. Кримінальний кодекс встановлює вичерпний перелік таких кримінальних правопорушень [10]. Щодо Кримінально Процесуального Кодексу, то в ньому питання кримінальних правопорушень у кіберпросторі врегульовано досить загально, на одному рівні з іншими кримінальними правопорушеннями, не враховуючи особливостей цього явища [11].

В Україні сьогодні існує Стратегія кібербезпеки України, затверджена відповідним Указом Президента. Як особливість слід відзначити, що в її змісті кіберпростір прирівняли до окремої сфери ведення бойових дій, на одному рівні з землею, повітрям чи морем [3].

Всі типи кримінальних правопорушень, зазначені у Кримінальному Кодексі України, визначаються розділом XVI – «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [10]. Пропонуємо коротко розглянути кожен тип кримінального правопорушення зазначеного розділу.

Стаття 361 – «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». Ця стаття передбачає втручання, яке призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу її обробки або порушення її маршрутизації [10].

Відповідно до статті 361 найпоширенішим кримінальним правопорушенням є злом, або несанкціоновані модифікації приладів чи програм.

Методів злому дуже багато, однак можна виділити основні, принцип роботи яких лежить в основі інших. Найпоширенішим методом є Bruteforce (Брутфорс). Поширення комп'ютерних вірусів – це ще один спосіб злому, який базується на розповсюдженні шкідливих програм, які здійснюють певні роботи з інформацією, в тому числі її викрадення та пересилання, що забезпечує доступ до різних приладів, систем і мереж. Поширення вірусів відбувається частково легальними шляхами, спочатку заражається якийсь файл, який Інтернет-користувачі самостійно завантажують на свої комп'ютери чи в системи, де з активацією файлу активується і сам вірус. Віруси, як метод злому, також є універсальними, але крім того, вони використовуються ще для ряду різних кримінальних правопорушень у кіберпросторі.

Стаття 361-1 – «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» [10]. Кримінальні правопорушення, передбачені цією статтею, стосуються нелегальних дій, пов'язаних зі шкідливими програмами або технічними засобами. Щодо шкідливих програм, то це комп'ютерні віруси. Віруси – це програми, які здатні самостійно множитись та поширюватись в системах, а крім того, виконують різні функції. Віруси бувають дуже різними за функціоналом та шкідливістю. Серед основних видів можна виділити декілька. Віруси-хробаки – програми, які багаторазово копіюють себе і тим самим засмічують комп'ютер, що погіршує його функціональність. Віруси-маскувальники приховують шкідливу активність та змінюють процеси в комп'ютерній системі, що полегшує дії зловмисників. Віруси-шпигуни збирають та пересилають різну інформацію про діяльність користувачів комп'ютерами, їх системами і мережами. Особливо небезпечними, особливо зараз, є два типи вірусів – локери і майнери. Локери – це віруси, які блокують доступ до комп'ютерної інформації або системи, після надсилають вимогу сплатити кошти за розблокування. Насправді більшість таких вірусів знищують інформацію і навіть виконання вимог від цього не рятує. Останній найвідоміший випадок масового поширення такого вірусу – це вірус Petya, який завдав значних збитків як Україні, так і країнам Балтії. Майнери – віруси які активно почали поширюватись після популяризації криптовалюти. Ці програми після проникнення в систему запускають процеси, які спрямовані на видобування електронної валюти, що дуже сильно навантажує системи і погіршує роботу техніки.

Стаття 361-2 – «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» [10]. Такі несанкціоновані дії з інформацією передбачають, що вони вчинені особою, яка не мала на це право, а також що доступ до інформації отримано нелегальним шляхом. Ця стаття більш чітко регулює питання витоку інформації. Збут інформації, тобто її продаж, має

кілька особливостей. Наприклад, інформація буває різною – службовою, таємною, особистою тощо, у відповідності до чого її збут може призвести до порушення диспозицій інших статей ККУ. Збут інформації – це також особливий вид її поширення, який передбачає комерційний умисел. Розповсюдження інформації стосується дій, які призвели до її витоку, у результаті чого до неї отримали доступ особи, які такого права не мали.

Стаття 362 – «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» [10]. Ця стаття є дуже неоднозначною, адже передбачає велику кількість можливих дій та наслідків, а особливо велике значення має форма вини. Якщо такі дії вчинені умисно, то наслідки будуть подібні до тих, що передбачені статтею 361 ККУ, тобто це виток, втрата, підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації. Такі дії також можуть бути близькі за змістом до інших кримінальних правопорушень у кіберпросторі, а крім того, можуть бути направлені на їх вчинення, наприклад використання комп'ютера для втручання в роботу іншого комп'ютера тощо. Більш складне питання, якщо такі дії вчинені з необережності. Тобто відповідно до нинішньої диспозиції статті, приміром, якщо працівник якоїсь компанії, яка має локальну мережу, через необережність допустив потрапляння вірусу-локера на комп'ютер з Інтернету, у результаті чого були уражені всі комп'ютери компанії, що завдало значних збитків, то відповідальність повинен нести саме працівник, а не зловмисники, які поширили цей вірус. Тут же виникають питання до компанії стосовно їх методів захисту від шкідливих програм тощо, а вирішення справи залежить від ряду інших об'єктивних обставин, незважаючи на спеціальний суб'єкт цього кримінального правопорушення.

Стаття 363 – «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється» [10]. Ця стаття передбачає дії, пов'язані з нелегальним використанням комп'ютерної електроніки, систем та мереж. В основному це стосується саме дій, які направлені на вчинення інших кримінальних правопорушень у кіберпросторі, або кримінальних правопорушень з використанням кіберпростору. До таких дій належить, наприклад, умисне розповсюдження шкідливих програм, втручання в роботу (злом) інших приладів, систем чи мереж, нелегальне поширення інформації тощо. Особливе місце займає питання порушення порядку чи правил захисту інформації, яке може виражатися у «піратстві», тобто порушенні авторських і суміжних прав на інформацію в кіберпросторі.

Стаття 363-1 – «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» [10]. Як і у статті 363, всі дії пов'язані з порушенням правил експлуатації, однак стаття 363-1 окремо виділяє конкретні дії, які направлені на перешкоджання функціонування інших комп'ютерних приладів, їх систем і мереж. Найпоширенішим такими кримінальними правопорушеннями є DDoS (дудос) атака – дії, спрямовані на перенавантаження окремої лаки кіберпростору (комп'ютера, сайту, або сервера) шляхом перевищення мережевих запитів, тобто перевантаження системи інформацією, що може вповільнити її роботу або повністю вивести з ладу. Для реалізації такої атаки використовують велику кількість техніки, однак часто ця техніка не належить хакеру.

На перший погляд, питання кримінальних правопорушень у кіберпросторі достатньо врегульоване, однак саме питання протидії має декілька серйозних прогалин, більшою мірою це стосується саме недосконалості кримінального процесу. Сьогодні ця правова сфера активно розвивається, реформи направлені на посилення правового забезпечення кібербезпеки та протидії кримінальних правопорушень у кіберпросторі.

Сьогодні в Україні, як і в світі в цілому, рівень кібербезпеки явно недостатній. Звісно, міжнародна співпраця сприяє вирішенню цієї проблеми, однак найважливіші дії повинні бути здійснені в середині країни, щоб згодом передати світу наш успішний досвід боротьби з кіберзлочинністю і регулювання кіберпростору. Для цього держава і суспільство повинно об'єднати свої зусилля та зробити все можливе для подолання проблеми кіберзлочинності. Реформи, які тривають сьогодні, повністю виправдані і є необхідними, однак в ідеалі правова сфера повинна враховувати не лише економічні та соціальні аспекти кіберзлочинності, а і технічні, особливо в питаннях процесуального законодавства.

Стрімкий розвиток інформаційних технологій та інформатизації суспільства призвів до появи нових видів кримінальних правопорушень і загроз – таких, як кіберзлочинність, кібертероризм, кібервійна. Російська Федерація тривалий час проводить інформаційну політику, спрямовану на формування негативного іміджу країн Балтії на міжнародній арені. Як свідчить порівняльний аналіз російськомовного контенту в інформаційному просторі прибалтійських країн, до цієї діяльності, окрім працівників сфери масової комунікації, залучені також відомі російські науково-дослідні інституції та окремі представники наукової громадськості. Зокрема, у щорічному звіті Поліції безпеки Латвії за 2017 р. відмічається посилення діяльності спецслужб РФ у російськомовному середовищі під гаслом захисту прав співвітчизників. Ця тенденція зберігається й у наступні 2017–2018 роки: у звіті за 2019 р. відзначається високий рівень активності спецслужб РФ, зокрема зацікавленість питаннями безпеки й оборони країни, суспільними процесами, діяльністю НАТО на території Латвії, відносинами між окремими етнічними групами тощо. Окрім цього, латвійські спецслужби вкотре спостерігають помітну активізацію діяльності в російськомовному молодіжному середовищі.

У Щорічнику Естонського департаменту інформації «International Security and Estonia» [12] стверджується, що РФ здійснює інформаційні кампанії проти країн-членів НАТО та ЄС шляхом поширення деструктивної інформації за допомогою ЗМІ та соціальних мереж. Росія послідовно поширює тезу, що Естонія, Латвія і Литва не поважають права своїх російськомовних мешканців і фальсифікують історію. Балтійським країнам створюється імідж недемократичних і проблемних партнерів з метою послаблення їхнього зв'язку із союзниками та скорочення їхньої ролі у формуванні зовнішньої політики щодо Росії.

У звіті Департаменту державної безпеки Литви за 2017 р. ідеться про розповсюдження неприйнятної для цієї держави інформації, ведення розвідки з території РФ і Республіки Білорусь (далі – РБ), спрямованої на військову та інші інфраструктури країни, електронної розвідки та кібернетичного шпіонажу.

Підсумовуючи вищевикладене, зазначимо, що основною загрозою національній безпеці країн Балтії є пропагандистська діяльність РФ в інформаційній сфері та її деструктивна діяльність в інформаційному просторі. Слід зауважити, що неодноразові спроби російських науковців переписати історію країн Балтії, фальсифікація та пропаганда нагадують російський сценарій напередодні анексії Кримського півострова та військової агресії на сході України.

Варто відмітити, що законодавство з кібербезпеки як країн Балтії, так і України визначає, що суб'єктами забезпечення кібербезпеки є не лише державні органи, а і недержавні організації та інші фізичні і юридичні особи. Крім того, жоден із нормативних актів зазначених держав не забороняє участі осіб у формуванні безпечного кіберпростору та власної кіберзахищеності. Відповідно до цього можна виділити державні і недержавні способи протидії кіберзлочинності.

Говорячи про роль недержавних організацій і суспільства в цьому питанні боротьби з кіберзлочинністю, бачимо, що основна роль – це саме попередження кримінальних правопорушень у кіберпросторі шляхом створення більш безпечного кіберпростору. Головне завдання суспільства – це обережність. Важливо, щоб користувачі сучасних технологій дотримувались всіх необхідних правил поведінки в мережі, серед яких: використання захисного програмного забезпечення і легальних ліцензованих програм, обережне використання Інтернет-ресурсів, контроль за особистими даними в мережі тощо. Крім підвищення загального рівня безпечності мережі, це також може сприяти зменшенню чисельності появи нових кіберзлочинців, а обережність користувачів кіберпростору ускладнить їхню діяльність [13].

Ураховуючи той факт, що інформаційні технології, що існують на даний момент, дозволяють як приховувати розташування, так і використовувати дані інших, то, на нашу думку, слід зробити такі кроки для забезпечення профілактики кіберзлочинів в країнах Балтії та України. Зокрема, на міжнародному рівні, на нашу думку, варто: 1) виробити і впровадити міжнародні угоди у сфері запобігання та розслідування кіберагресії; 2) створити міжнародний орган з регіональними представництвами. Цей орган повинен бути еквівалентом ООН у кіберпросторі.

На національному рівні кожній із розглянутих країн пропонуємо: 1) брати участь у розробці міжнародної стратегії з протидії кіберзагрозам і створенні єдиних міжнародно-правових механізмів регулювання віртуального простору; 2) розробити проект Національної Концепції Стратегії кібербезпеки держави, яка повинна бути заснована на принципах і законах інших державних документів, які б розглядали її реалізацію на різних національних рівнях і сферах; 3) нарощувати потужності

в інформаційній сфері з протидії електронним атакам. Необхідно посилити заходи внутрішньополітичного характеру щодо стимулювання розвитку технологічної складової частини кібербезпеки для збереження балансу сил і складання противаги іншим імовірнісним «супротивникам» в області кібербезпеки; 4) виступати, впроваджувати і реалізувати регіональне, міжнародне співробітництво у сфері кібербезпеки, відстеження діяльності кримінально протиправних, терористичних груп та окремих хакерів, які діють в кіберпросторі; 5) виступати і брати активну участь у розвитку міжнародного співробітництва в області і структурах, спрямованих на виявлення кіберзагроз, своєчасно виявляти, запобігати, захищати, а також мінімізувати наслідки.

**Висновок.** Основні напрямки протидії кіберзлочинності націлені на вирішення проблем, пов'язаних із розширенням законодавства, виробленням заходів попередження і зниженням рівня латентності кримінальних правопорушень, що здійснюються в кіберпросторі. Однак вже сьогодні, в умовах викликів і загроз XXI століття, необхідно обговорювати і вирішувати проблеми, які ставлять перед кримінальної політикою нові технології. Аналізуючи вищенаведені види кримінальних правопорушень у кіберпросторі, стає очевидною необхідність їх попередження. Іноді вчинення навіть не дуже серйозного кримінального правопорушення може призвести до небезпечних наслідків, які бути можуть і непоправними. Законодавчій системі країн Балтії та України доцільніше було б вжити заходів посилення санкцій статей окремих складів кримінально караних кримінальних правопорушень, що мають відношення до кримінальних правопорушень у кіберпросторі. Таким чином, вважаємо, що з метою протидії кримінальним правопорушенням, скоєним із використанням сучасних інформаційних технологій, нашій державі слід постійно підвищувати безпеку інформаційних систем, розвивати сучасні інформаційні технології, удосконалювати законодавство у сфері інформаційних кримінальних правопорушень, розвивати конкурентоспроможні засоби інформатизації, розширювати міжнародне співробітництво у сфері безпечного використання інформаційних ресурсів.

**Література**

1. Maria Claudia Menezes Leal Nunes. Cyberspace: the challenges of norm formation. Revista Conjuntura Global v. 10, n. 1. 2021. P. 178–194. DOI: 10.5380/cg.v10i1.78424. URL: https://revistas.ufpr.br/conjgloblal/article/viewFile/78424/44108 (дата звернення: 20.11.2022).

2. Report of the X UN Congress on the prevention of crime and the treatment of offenders. (2000). URL: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf. (дата звернення: 20.11.2022).

3. Про основні засади забезпечення кібербезпеки України : Закон України № 2163-VIII від 05.10.2017 р. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.11.2022).

4. Конвенція про кіберзлочинність Рада Європи; Конвенція, Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 20.11.2022).

5. Newmeyer, K.P. Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*, 1(3): 9-19. 2015

6. Стратегічна безпека Естонської Республіки. URL: https://www.mkm.ee/ (дата звернення: 20.11.2022).

7. Офіційний сайт журналу єврогід. URL: https://www.eurodig.org/ (дата звернення: 20.11.2022).

8. Par pamatnostādnēm 'Latvijas kiberdrošības stratēģija 2014.-2018.gadam'. URL: https://likumi.lv/doc.php?id=263912 (дата звернення: 20.11.2022).

9. Міністерство Юстиції України: правове регулювання інтернет – засобів масової інформації. URL: https://minjust.gov.ua/m/str_24640 (дата звернення: 20.11.2022).

10. Кримінальний кодекс України від 5 квітня 2001 року. *Відомості Верховної Ради України*. 2001. № 25-26. URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 20.11.2022).

11. Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI: URL: http://zakon3.rada.gov.ua/laws/show/4651-17 (дата звернення: 20.11.2022).

12. Official website International Securityand Estonia. URL: https://www.valisluureamet.ee/ (дата звернення: 20.11.2022).

13. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. Безпечне місто. URL: http://safe-city.com.ua/kiberzlochynnist-u-vsih-yiyi-proyavah-vydy-naslidky-ta-sposoby-borotby/ (дата звернення: 20.11.2022).

***Думчиков М. О.,***
*кандидат юридичних наук,*
*старший викладач кафедри кримінально правових дисциплін та судочинства*
*Навчально-наукового інституту права*
*Сумського державного університету*